LANDSAT DATA CONTINUITY MISSION

GROUND SYSTEM
Mission Operations Element

MISSION ASSURANCE
REQUIREMENTS
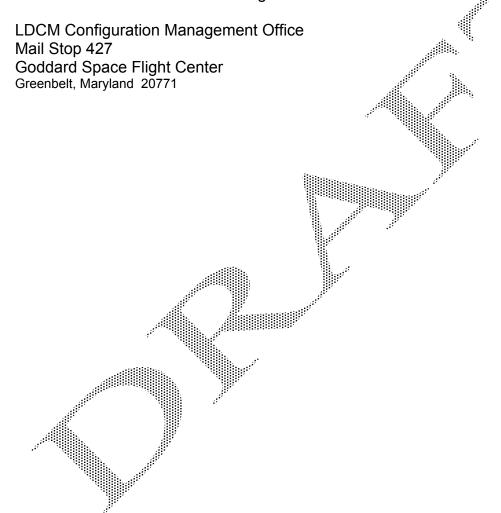
October 21, 2007

Goddard Space Flight Center
Greenbelt, Maryland

National Aeronautics and

CM FOREWORD

This document is a Landsat Data Continuity Mission (LDCM) Project Configuration Management (CM)-controlled document. Changes to this document require prior approval of the applicable Configuration Control Board (CCB) Chairperson or designee. Proposed changes shall be submitted to the LDCM CM Office (CMO), along with supportive material justifying the proposed change. Changes to this document will be made by complete revision.

Questions or comments concerning this document should be addressed to:

LDCM Configuration Management Office
Mail Stop 427
Goddard Space Flight Center
Greenbelt, Maryland 20771

Signature Page

Prepared by:

Patricia A. Huber LDCM Chief Safety and Mission Assurance Officer NASA GSFC Code 323	Date

Reviewed by:

Vicki Dulski LDCM Ground Systems Manager NASA/GSFC – Code 581	Date	Doug Daniels LDCM Ground Systems Lead Aerospace contractor to USGS/EROS	Date

Approved by: **Approved by:**

William R. Ochs LDCM Project Manager NASA/GSFC – Code 427	Date	Mike Headley LDCM Project Manager USGS/EROS	Date

LDCM PROJECT
DOCUMENT CHANGE RECORD

Sheet: 1 of 1

REV LEVEL	DESCRIPTION OF CHANGE	APPROVED BY	DATE APPROVED

TABLE OF CONTENTS

1.0 GENERAL

This document, referred to as the "Ground System MAR," defines the Safety and Mission Assurance (S&MA) requirements for the LDCM Ground System (GS). Additional mission assurance requirements are defined in the Ground System and Element requirements documents and any cooresponding Statements of Work (SOWs) for out-of-house development efforts.

References to the "developer" in this document are directed to the developer of LDCM GS elements. References to the "CSO" refer to the NASA GSFC LDCM Project Chief Safety and Mission Assurance Manager. References to the "Government" or the "LDCM Project Office" refer to the NASA GSFC and USGS/EROS LDCM Project Offices.

The developer shall create a Software Assurance Plan (SAP) that provides a comprehensive plan for accomplishing the S&MA activities in compliance with the requirements herein. The SAP shall describe the developer's system for planning, documentation, and controls that will ensure complete traceability through all phases of the design, implementation, test, and operation of deliverable items. The developer's SAP shall be delivered as part of Software Development and Management Plan (MOE CDRL MO-9).

The SAP shall include:

a. An overview of the developer's plan for accomplishing the assurance activities required by the GS MAR.
b. Specific and detailed description of how the performance assurance requirements are to be accomplished. Referenced documents that provide the required details shall be included with the SAP.
c. The rationale for any planned noncompliance to the GS MAR including the details of the developer's alternate approach, if any, to meet the specific GS MAR requirement

1.1 Scope

The requirements stated in this attachment apply to all work accomplished by the GS developer and their subcontractors.

1.2 Applicable Documents (Section 3.0)

To the extent referenced herein, applicable portions of the documents listed in Section 3.0 form a part of this document (i.e., the LDCM GS MAR). The latest version of each document, at the time of the issue of this document, is applicable. In the event of a conflict between the documents listed in Section 3.0 and this requirements specification, the contents of this specification shall be considered the superseding requirements. In

the event of a conflict between this Mission Assurance Requirements document and a Statement of Work (SOW), the SOW shall take precedence. In the event of any other unresolved conflict associated with out-of house procurements, the contracting officer shall be notified, and the order of precedence will be as directed by the contracting officer. In the event of conflicts associated with other GS development, the Ground System Manager shall be notified, and the order of precedence will be as determined by the Ground System Manager.

1.3 Acronyms (Section 4.0)

Section 4.0 defines the acronyms used in this document.

1.4 Overall System Safety and Mission Assurance (S&MA) Requirements

The developer is required to plan and implement an organized S&MA Program that encompasses all ground system software and hardware critical for mission success.

Managers of the developer assurance activities shall have direct access to developer management independent of project management, with the functional freedom and authority to interact with all other elements of the project. Issues requiring project management attention shall be addressed with the developer(s) through the GS and Project Manager(s) and/or Contracting Officer Technical Representative(s) (COTR).

1.5 Surveillance of Developer

The work activities, operations and documentation performed by the developer and/or his suppliers are subject to evaluation, review, audit, and inspection by Government-designated representatives from GSFC and USGS/EROS, the Government Inspection Agency (GIA), or an independent assurance contractor (IAC). The developer and/or suppliers shall grant access for LDCM Project and/or LDCM Project representatives to conduct an assessment/survey upon notice. Resources shall be provided to assist with the assessment/survey with minimal disruption to work activities. The developer, upon request, shall provide government assurance representatives with the documents, records, and equipment required to perform their S&MA activities. The developer shall also provide the government assurance representative(s) with an acceptable work area within developer facilities.

1.6 S&MA-Related Deliverables

All deliverable documents required by this MAR are listed in the NASA-USGS Project Implementation Agreement (TBR) and the LDCM Mission Operations Element Contract Data Requirements List (GSFC 427-09-02).

2.0   Ground System Assurance Requirements

GS elements may include but are not limited to GS software, firmware and hardware, ground support elements (simulators, etc), Commercial Off The Shelf (COTS), databases, key parameter and test checkout software, and any software developed under the project that is related to flight mission operations. These elements may be developed in-house entirely by the developer, provided by a sub-developer/subcontractor to the developer, purchased by the government, purchased by the developer, or furnished by other parties including the government.

2.1   Quality Management System

The developer shall have a Quality Management System (QMS) that is compliant with American National Standards Institute (ANSI)/American Society for Quality (ASQ) Q9001 or equivalent. In all cases the development effort shall provide evidence (quality records for Government review) as insight to the quality of the developing software, hardware and other GS components as evidence of application of QMS processes, and as status of assurance problems, safety issues and organizational/personnel changes. Quality records shall include any corrective actions, relating to GS development, recommended by QMS audits. The developer will allow Government audits, when deemed necessary by the Project Manager, to assure compliance of the developer's QMS with ANSI/ASQ Q9001 and to assure that the QMS is applied to the contracted activities. The developers Quality Manual shall be made available to the Government.

The developer shall maintain/possess a QA organization/entity that is assigned the responsibility to monitor the development process, and the associated components/products. QA shall interface with all relevant disciplines participating in the lifecycle activities including engineering, configuration management and testing. The QA group is empowered to alert project management to effect changes to the program when quality goals are not being met.

The developer shall provide for measuring and monitoring the performance of the program's defined management and development processes. The developer shall verify adherence to the defined development and management processes. The developer shall perform audits on designated work products to verify compliance with quality goals and adherence to the applicable standards and requirements. The developer shall identify training to be performed.

The developer shall plan and document software development processes and procedures, software tools, resources, and deliverables throughout the lifecycle. A Software Development Plan (SDP) shall be delivered by the developer (MOE CDRL MO-9).

2.2   Requirements

The developer shall identify, document and maintain GS element requirements that will serve as the basis of the development, implementation, operation and maintenance of the GS and its elements. These requirements shall include but are not limited to functional, performance, reliability, maintainability, safety and test/verification requirements.

The developer shall work with the Government and/or other entities as necessary to resolve any problems/issues associated with the GS requirements.

The developer shall baseline the GS element requirements early in the development effort, specifically in conjunction with a formal requirement review. The developer shall maintain the GS element requirements under configuration control throughout the lifecycle. All changes to the GS element requirements, including those generated both internally and externally, shall be managed by the developer's Configuration Control Board (CCB) process and reviewed/approved as applicable by GSFC.

GS element requirements shall be delivered to the Government (MOE CDRL MO-3).

2.3 Reviews

The developer shall implement a program of engineering reviews (peer reviews) throughout the development lifecycle to identify and resolve concerns prior to formal, system level reviews.

The developer shall conduct a program of planned, scheduled, and documented system level reviews. GS and element review packages shall be delivered to the Government (MOE CDRL RE-7).

2.4 Assurance Activities

The developer shall perform various assurance-related activities throughout the development lifecycle to ensure that the GS and its elements meet GS/element requirements. The developer shall initiate these activities as early in the development lifecycle as possible, specifically in the concept phase, and continue these activities into the operations and maintenance phase where applicable. Some of these assurance-related activities are applicable to all phases of the lifecycle and the developer shall conduct these activities throughout the entire lifecycle.

2.5 Requirements Phase

Specific assurance-related activities that the developer shall perform during the requirements phase include but are not limited to the following (Note: Some of these activities may be performed prior to this phase or subsequent to this phase where applicable):

a. Analyze and refine the requirements to assure they are consistent, clear, valid, feasible, compatible, complete, testable and do not include inappropriate level of design information

b. Ensure requirements are generated, analyzed, refined, decomposed and allocated to appropriate GS elements through the use of a systems analysis and allocation process. This process shall be used to verify requirements are correct and complete at each level prior to further allocation and decomposition, and to verify them for feasibility and top-level design concept prior to further allocation.

c. Establish functional, performance, safety, reliability, maintainability and test/verification requirements for each incremental element delivery/build, as applicable. This process should assure all requirements are allocated to planned deliveries/builds prior to the design and development of the delivery/build.

d. Manage allocation of new and additional requirements between hardware, software and other components by a change review and control process; and manage the reallocation of existing requirements between hardware, software and other elements by a change review and control process

e. Use a defined process to generate, review and allocate interface requirements

f. Maintain a process to provide, ensure and maintain two-way requirements traceability from system specifications to hardware, software and other components that serve as configuration items. This requirement traceability shall be established and documented as early in the lifecycle as possible.

g. Generate, document and maintain a requirements verification matrix

h. Conduct a requirement review and at the end of each phase of the development process ensure requirements are complete and testable

2.6   Design Phase

Specific assurance-related activities that the developer shall perform during the design phase include but are not limited to the following (Note: Some of these activities may be performed prior to this phase as applicable.):

a. Maintain a process to define, maintain, and document interfaces (both internal and external) within the architecture

b. Allocate and maintain traceability between the GS architecture/elements and the GS requirements

c. Conduct design walkthroughs and reviews

d. Place the design under configuration control

2.7   Implementation Phase

Specific assurance-related activities that the developer shall perform during the implementation phase include but are not limited to the following (Note: Some of these activities may be performed prior to this phase as applicable):

a. Define, schedule, and document the components of each build, delivery and/or release

b. Conduct peer reviews/walkthroughs for code
c. Conduct unit testing
d. Conduct reviews and appropriate tests at the end of this phase of the development process to ensure that the requirements have been correctly implemented into design, code, documentation and data
e. Allocate and maintain traceability between the GS element architectures and the GS element requirements

2.8 Testing Phase

Specific assurance-related activities that the developer shall perform during the test phase include but are not limited to the following (Note: Some of these activities may be performed prior to this phase as applicable):

a. Plan for and document test related activities early in the development stages of the project in a test plan(s) (MOE CDRL MO-4). The plan shall be maintained under configuration control and updated as requirements are changed. All test plans shall be made subject to Government review and approval as applicable. The developer's test plans shall include but is not limited to the following:

1. Description of the tests to be performed including the different levels of testing (from units to Computer Software Configuration Items (CSCIs) to subsystem to system-level test), expected test results, personnel responsible for testing, any required support from other organizations and data required for the test(s)
2. GS components/elements to be tested
3. Test environment under which the test(s) will be conducted including test facility requirements, special test support tools (i.e., simulators, emulators, etc.) and any special operating conditions required
4. Requirements Verification Matrix (RVM) documenting traceability of requirements to test cases

b. Generate test procedures that implement the test plans and facilitate the verification and validation of GS requirements (MOE CDRL MO-5). All test procedures shall be made subject to Government review and approval as applicable.
c. Maintain a process to ensure that any test tools and test data are qualified prior to use during testing activities
d. Ensure that test personnel attend and participate as necessary in various reviews throughout the lifecycle, to include but not limited to requirements, architecture and design reviews
e. Identify and document test readiness criteria for formal testing activities. Test criteria shall be made subject to Government review and approval as applicable.
f. Maintain and update the RVM generated earlier in the lifecycle to include the status (pass, fail, deferred, etc) of each requirement throughout the testing phases and various testing activities

g. Test reports (MOE CDRL MO-6) should document the validation of requirements, specific tests completed, conformance of the test results to the expected results, the number, type and criticality of any identified discrepancies/nonconformances, identification of the hardware, software and other GS elements tested including version number, etc.

h. Document all defects/nonconformances encountered during the testing activities. These defects/nonconformances shall be assessed for criticality, severity, impact, etc to determine appropriate action and resolution. The developer shall track and report on the status of all defects/nonconformances.

i. Identify all nonconformances that impact the developer's ability to meet GS requirements and document these items in a waiver which must be reviewed/approved by the Government as applicable

j. Ensure and maintain configuration control of the test environment including hardware, software, simulators, test data, databases and other components throughout the test program

k. Assess all changes made to the system architecture and its components to determine the necessity for regression testing. The developer shall conduct regression testing based upon assessed and approved/implemented changes as appropriate.

l. Conduct contingency and off-nominal condition testing

m. Conduct pre-test briefings and generate briefing messages where appropriate to facilitate the coordination of various test related activities. Briefing message contents may include but are not limited to:

   1. Test Case/Procedure Name/Number
   2. Purpose of the Test
   3. Testing Dates/Times
   4. Test Participants and required resources (scheduling of lab and station support, data sources (e.g. s/c, s/c data tape, engineering test unit or s/c simulator), software, hardware and support system configurations (to include release/version numbers where appropriate)
   5. GS requirements to be verified
   6. Contact list to include names and numbers of test participants

n. Conduct post-test debriefings. During these debriefs, the developer shall summarize test results, disposition the test (pass/fail, etc), deviations from test procedures, requirements verified and discrepancy reports generated, etc.

o. Conduct mission simulations to validate nominal and contingency mission operating procedures and to provide for operator familiarization training. In order to provide ample time for checkout of operational configurations, it is considered essential that users participate in mission simulations. Ground operation procedures shall be delivered to the Government in accordance with the CDRL.

A System Performance Verification Plan (MOE CDRLs SE-6, MO-4), Performance Verification Procedures (MOE CDRL MO-5), and Verification Reports (MOE CDRLs SE-7, MO-6) shall be delivered to the Government.

2.9 Delivery Phase

Specific assurance-related activities that the developer shall perform during the delivery phase include but are not limited to the following (Note: Some of these activities may be performed prior to this phase as applicable):

1. System delivery letter (MOE CDRL MO-10):

    (a) Description of hardware and software delivery contents
    (b) Build instructions, including the source code, databases and all files required to complete a successful software build
    (c) Special operating instructions
    (d) List of resolved anomaly reports and change requests
    (e) List of unresolved anomaly reports and change requests
    (f) Copy of resolved anomaly reports and change requests
    (g) Copy of unresolved anomaly reports and change requests
    (h) Matrix of requirements addressed by this release, including waivers for those requirements not met as appropriate
    (i) List of changes to documentation associated with this release
    (j) Verification success criteria
    (k) Known problems and workarounds

2. Software delivery media
3. Accompanying documentation

Data delivery packages shall be delivered to the Government.

2.10 COTS, Existing and Purchased Software

If the developer will be provided software, or will use existing or purchased software and/or COTS products, the developer is responsible for these components meeting all functional, performance and interface requirements. Any significant modification to these components shall be subject to all of the provisions of the developer's QMS and the provisions of this document. Significant modification will be defined by the project and its CCB procedures and will be subject to Government review.

2.11 COTS Management

The developer shall identify and maintain traceability of GS and/or element requirements satisfied by COTS products/components and shall document the rationale/justification for the selection of all COTS components contained within the element. The developer shall ensure that the CM program covers all COTS/components.

The developer shall demonstrate and document the fulfillment of GS requirements by COTS products/components via the RVM.

2.12 Databases

The developer shall maintain a process and procedures for database development as appropriate. The process shall include activities such as internal reviews, walkthroughs, statusing, test, and discrepancy resolution.

The developer shall utilize a process for the verification and validation of the database system.

The developer shall ensure that system/software releases and database releases are configured with one another.

The developer shall implement CM on the database system to ensure that the database release version is defined and documented, controlled and that the integrity of the data contained within is controlled.

The developer shall ensure that appropriate security measures are implemented on the database system and on the data contained within the database system.

2.13 Security Assurance

The developer shall conduct a security program to identify and mitigate security risks associated with the GS and its elements. All security risks shall be assessed/analyzed for impact and likelihood of occurrence. The security program shall ensure that security requirements are established, documented and implemented during all phases of the software lifecycle. Security tasks and activities shall include the addressing of security concerns during reviews, analyses, inspections, testing and audits.

The developer shall identify and characterize system security vulnerabilities to include analyzing GS assets/elements, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability. The developer shall identify and report upon all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security.

The developer shall ensure that solutions are verified and validated with respect to security.

The developer shall be compliant with all NASA and USGS security related policies, procedures, standards and guidelines.

2.14 Electromagnetic Compatibility Control

The developer shall demonstrate that GS equipment is not affected by electromagnetic compatibility problems nor does it pose a threat to other equipment.

2.15 Reliability, Availability, and Maintainability

Reliability, availability and maintainability assurance requirements for the GS and associated elements shall include the following:

a. Starting in the conceptual design stage the developer shall clearly define, based upon LDCM mission success criteria and reliability requirements, levels of performance. The developer shall establish and implement specific design criteria needed to mitigate unacceptable levels of performance. Design criteria shall be accessible for Government review.

b. Based on the definition of acceptable levels of performance, the developer shall define the following minimum acceptable maintainability parameters:

1. Diagnostic time to detect and fault isolate to the defective Line Replacement Unit (LRU)
2. Time required to remove and replace the defective LRU
3. Time required to complete checkout and restore operational status

c. The developer shall assure that equipment and components obtained from COTS vendors meet allocated requirements and if not, such deficiencies shall be reported to the Government.

d. The developer shall develop and implement specific design criteria to facilitate maintenance or repair actions. In establishing maintainability design criteria that meets the specification, the contractor shall use data obtained from similar system installations. Design criteria shall include design for modularity, optimum accessibility, accurate fault diagnostics, standardization, and commonality. Design criteria shall be accessible for Government review.

2.16 Risk Management

The developer shall implement a Continuous Risk Management System (CRMS) that provides for the identification, analysis, tracking, communication, resolution, mitigation and retirement of mission risks. Risk management applies to all software and hardware products, components and processes. The developer shall:

a. Search for, locate, identify and document reliability and quality risks before they become problems.
b. Evaluate, classify and prioritize all identified reliability and quality risks.
c. Develop and implement risk mitigation strategies, actions and tasks and assign appropriate resources.

d. Track risks being mitigated; capture risk attributes and mitigation information by collecting data; establish performance metrics; and examine trends, deviations and anomalies.
e. Control risks by performing risk close-out, re-planning, contingency planning, or continued tracking and execution of the current plan.
f. Communicate and document (via the risk recording, reporting, and monitoring system) risk information to ensure it is conveyed between all levels of the project.
g. Report on outstanding risk items at all management and design reviews. The GSFC Project Office, the GSFC Systems Review Office (SRO) (for design reviews only), and the developer will agree on what level of detail is appropriate for each review.

The developer shall develop a Risk Management Plan (MOE CDRL PM-12). The plan shall include risks associated with hardware (technical challenges, new technology qualification, etc), software, COTS, system safety, performance and programmatic risks (cost and schedule). The plan shall identify which tools and techniques will be used to manage the risks. The risk areas that are identified shall be addressed at the peer reviews and at other appropriate milestone reviews. All identified reliability and quality risks shall be documented and reported in accordance with the NASA and USGS Risk Management Plans. Risk status shall be available to the Project for review. The status of risks shall also be provided in technical review reports. Although not all risks will be fully mitigated, all risks shall be addressed with mitigation and acceptance strategies agreed upon at appropriate mission reviews.

2.17 Software Configuration Management

The developer shall maintain a Software Configuration Management (SCM) system that provides control of changes to software products, beginning in the requirements phase and continuing until government acceptance.

The developer shall ensure the configuration management system addresses baseline control, configuration identification, configuration control, configuration status accounting and configuration authentication. The developer shall describe the SCM system in a SCM Plan that is delivered the the Government (MOE CDRL PM-10).

2.18 System Safety

The developer shall initiate a safety program to identify and mitigate safety critical GS elements. If any GS element(s) are identified as safety critical, the developer shall conduct a safety program on those components in compliance with NPG 8715.3, "NASA Safety Manual". For GS elements that are software and deemed as safety critical, the safety program shall be implemented in accordance with NASA-STD-8719.13A "NASA Software Safety Standard". The developer shall establish and identify procedures and instructions, which will be used to execute all system safety analyses.

2.19 Problem Reporting and Corrective Action

The developer shall implement a process for Problem Reporting and Corrective Action that addresses reporting, analyzing and correcting nonconformances throughout the development lifecycle. The developer's QMS shall provide for a corrective action process that tracks every nonconformance to its final disposition.
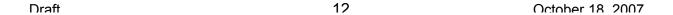
The Problem Reporting system and Corrective Action process shall include:

a. Nonconformance detection and reporting procedures.
b. Nonconformance tracking and management procedures.
c. Nonconformance impact assessment and corrective action procedures.
d. Interfaces to the Configuration Management process.

2.20 Independent Verification and Validation (TBR)

The developer shall provide all information required for the IV&V effort to NASA IV&V personnel. This includes, but is not limited to, access to all software reviews and reports, developer plans and procedures, software code, software design documentation, and software problem reporting data. Wherever possible, the developer shall permit electronic access to the required information or furnish soft copies of requested information to NASA IV&V personnel.

The developer shall review and assess all NASA IV&V findings and recommendations. The developer shall forward their assessment of these findings and recommendations to NASA IV&V personnel accordingly. A developer Point of Contact shall be assigned and available to NASA IV&V personnel for questions, clarification, and status meetings, as needed.
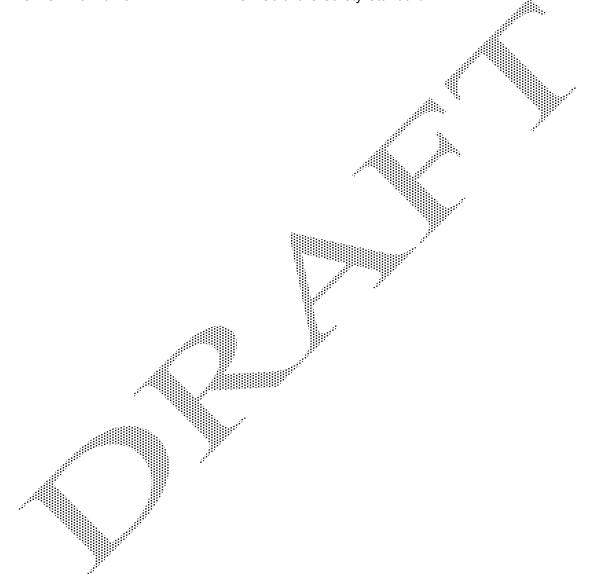
3.0 Referenced Documents

ANSI/ISO/ASQ Q9001: 2000   American National Standard Quality Systems - Model for Quality Assurance in Design, Development, Production, Installation and Servicing

NASA-STD 8719.13A   NASA Software Safety Standard

4.0 Acronyms

ANSI	American National Standards Institute
ASQ	American Society for Quality
CCB	Configuration Control Board
CCR	Configuration Change Request
CDR	Critical Design Review
CDRL	Contract Delivery Requirement List
CIL	Critical Items List
CM	Configuration Management
COTR	(GSFC LDCM) Contracting Officer's Technical Representative
COTS	Commercial Off The Shelf
CRMS	Continuous Risk Management System
CSCI	Computer Software Configuration Items
CSO	(GSFC LDCM) Chief Safety and Mission Assurance Officer
DBMS	Database Management System
DID	Data Item Description
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCA	Functional Control Audit
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects and Criticality Analysis
GS	Ground System
GFE	Government Furnished Equipment
GIA	Government Inspection Agency
GSFC	Goddard Space Flight Center
IAC	Independent Assurance Contractor
ICD	Interface Control Document
IOC	In-Orbit Checkout
IV&V	Independent Verification and Validation
L&EO	Launch and Early Orbit
LDCM	Landsat Data Continuity Mission
LRU	Line Replacement Unit
MAR	Mission Assurance Requirements (Document)
MOC	Mission Operations Center
ORR	Operation Readiness Review
PCA	Physical Control Audit
PDR	Preliminary Design Review
PSR	Pre-Shipment Review
QA	Quality Assurance
QMS	Quality Management System
RVM	Requirements Verification Matrix
SAP	Software Assurance Plan
S&MA	System Safety and Mission Assurance
SCM	Software Configuration Management
SDP	Software Development Plan
SOW	Statement of Work
SRO	Systems Review Office
SRR	System Requirements Review